

10 / 567 202

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/016450

International filing date: 07 September 2005 (07.09.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-298243
Filing date: 12 October 2004 (12.10.2004)

Date of receipt at the International Bureau: 13 October 2005 (13.10.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

BEST AVAILABLE COPY



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2 0 0 4 年 1 0 月 1 2 日

出 願 番 号
Application Number: 特 願 2 0 0 4 - 2 9 8 2 4 3

パリ条約による外国への出願
に用いる優先権の主張の基礎
となる出願の国コードと出願
番号

The country code and number
of your priority application,
to be used for filing abroad
under the Paris Convention, is

J P 2 0 0 4 - 2 9 8 2 4 3

出 願 人
Applicant(s): 日 本 電 信 電 話 株 式 有 限 公 司

2 0 0 5 年 9 月 2 8 日

特許庁長官
Commissioner,
Japan Patent Office

中 嶋



【書類名】 特許願
【整理番号】 NTTH165995
【提出日】 平成16年10月12日
【あて先】 特許庁長官殿
【国際特許分類】 H04L 12/56
H04L 12/46
【発明者】
【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内
【氏名】 佐竹 康宏
【発明者】
【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内
【氏名】 長島 雅夫
【特許出願人】
【識別番号】 000004226
【氏名又は名称】 日本電信電話株式会社
【代理人】
【識別番号】 100089118
【弁理士】
【氏名又は名称】 酒井 宏明
【選任した代理人】
【識別番号】 100114306
【弁理士】
【氏名又は名称】 中辻 史郎
【手数料の表示】
【予納台帳番号】 036711
【納付金額】 16,000円
【提出物件の目録】
【物件名】 特許請求の範囲 1
【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1
【包括委任状番号】 0310351

【書類名】 特許請求の範囲

【請求項 1】

ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在するゲート装置若しくは前記中継装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御方法であって、

前記ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報を前記ゲート装置が取得する正規アドレス情報取得工程と、

前記正規アドレス情報取得工程により取得された正規アドレス情報に基づいて前記ゲート装置が非攻撃パケットの条件を示す正規条件情報を生成する正規条件情報生成工程と、

前記ゲート装置が前記ネットワークから受信したパケットのうち前記正規条件情報生成工程により生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうパケットの通過を制限するパケット制限工程と

を含んだことを特徴とするサービス不能攻撃防御方法。

【請求項 2】

前記正規アドレス情報取得工程は、前記ゲート装置が前記中継装置に対して自装置のアドレス情報を通知するアドレス情報通知工程と、前記中継装置が前記正当な装置からの正規アドレス情報を受信した場合に、前記アドレス情報通知工程により通知された前記アドレス情報に基づいて当該正規アドレス情報を前記ゲート装置に対して中継する正規アドレス情報中継工程と、前記ゲート装置が前記正規アドレス情報を受信する受信工程とを含んだことを特徴とする請求項 1 に記載のサービス不能攻撃防御方法。

【請求項 3】

前記アドレス情報通知工程は、前記ゲート装置のアドレス情報を通知された中継装置が隣接する他の中継装置に前記ゲート装置のアドレス情報を中継し、前記正規アドレス情報中継工程は、前記他の中継装置が前記正当な装置からの正規アドレス情報を受信した場合に、前記ゲート装置のアドレス情報に基づいて隣接する中継装置若しくは前記ゲート装置に前記正規アドレス情報を中継することを特徴とする請求項 2 に記載のサービス不能攻撃防御方法。

【請求項 4】

前記正規アドレス情報取得工程は、正規アドレス情報を一括管理する正規アドレス情報提供装置が前記正規アドレス情報を各正当な装置から受信して格納する正規アドレス情報格納工程と、前記正規アドレス情報提供装置が前記ゲート装置から前記正規アドレス情報の送信要求を受け付けた場合に、送信要求された正規アドレス情報を前記ゲート装置に対して通知する正規アドレス情報通知工程と、前記ゲート装置が前記正規アドレス情報を受信する受信工程とを含んだことを特徴とする請求項 1 に記載のサービス不能攻撃防御方法。

【請求項 5】

前記正規アドレス情報取得工程は、アドレスを発行するアドレス発行装置若しくは正当な認証を受けた通信機器を前記ネットワーク上に所在する正当な装置により送信された前記正規アドレス情報を前記ゲート装置が取得することを特徴とする請求項 1 ～ 4 のいずれか一つに記載のサービス不能攻撃防御方法。

【請求項 6】

前記ゲート装置が前記ネットワークから受信されたパケットによる攻撃を検知する攻撃検知工程と、前記攻撃検知工程により攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成する容疑シグネチャ生成工程と、前記正規条件情報生成工程により生成された正規条件情報を正規条件情報記憶部に格納する正規条件情報格納工程と、前記容疑シグネチャ生成工程により生成された容疑シグネチャに該当するパケットのうち、前記正規条件情報に示された条件に適合するパケットの特徴を表す正規シグネチャを生成する正規シグネチャ生成工程とをさらに含み、前記パケット制限工程は、前記容疑シグネチャ生成工程により生成された容疑シグネチャおよび前記正規シグネチャ生成工程により生成された正規シグネチャに基づいて前記ネットワークから受信したパケットの通過を制限することを

特徴とする請求項 1～5 のいずれか一つに記載のサービス不能攻撃防御方法。

【請求項 7】

前記容疑シグネチャ生成工程により生成された容疑シグネチャおよび前記正規シグネチャ生成工程により生成された正規シグネチャを前記ゲート装置が前記中継装置に通知するシグネチャ通知工程と、前記中継装置が前記シグネチャ通知工程により通知された容疑シグネチャおよび正規シグネチャに基づいてバケットの通過を制限制御するバケット制限制御工程とをさらに含んだことを特徴とする請求項 6 に記載のサービス不能攻撃防御方法。

【請求項 8】

ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在し、前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御装置であって、

前記ネットワーク上に所在する正当な装置により送信された非攻撃バケットの送信元を示す正規アドレス情報を取得する正規アドレス情報取得手段と、

前記正規アドレス情報取得手段により取得された正規アドレス情報に基づいて非攻撃バケットの条件を示す正規条件情報を生成する正規条件情報生成手段と、

前記ネットワークから受信したバケットのうち前記正規条件情報生成手段により生成された正規条件情報に示された条件に適合するバケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうバケットの通過を制限するバケット制限手段と

を備えたことを特徴とするサービス不能攻撃防御装置。

【請求項 9】

前記正規アドレス情報取得手段は、前記中継装置に対して自装置のアドレス情報を通知するアドレス情報通知手段と、前記アドレス情報通知手段により通知した自装置のアドレス情報に応答して前記中継装置が返送した前記正当な装置からの正規アドレス情報を受信する受信手段とを備えたことを特徴とする請求項 8 に記載のサービス不能攻撃防御装置。

【請求項 10】

前記正規アドレス情報取得手段は、正規アドレス情報を一括管理する正規アドレス情報提供装置に対して前記正規アドレス情報の送信要求をおこなう正規アドレス情報送信要求手段と、前記正規アドレス情報の送信要求に応答して返送された正規アドレス情報を受信する受信手段とを備えたことを特徴とする請求項 9 に記載のサービス不能攻撃防御装置。

【請求項 11】

サービス不能攻撃対象となる通信機器に対するサービス不能攻撃を防御するゲート装置および／またはネットワークを形成する一または複数の中継装置と接続された中継装置であって、

前記ゲート装置のアドレス情報を取得するアドレス情報取得手段と、

前記ネットワーク上に所在する正当な装置により送信された非攻撃バケットの送信元を示す正規アドレス情報を受信した際に、前記アドレス情報取得手段により取得されたアドレス情報に基づいて、前記ゲート装置または隣接する他の中継装置に前記正規アドレス情報を中継する正規アドレス情報中継手段と

を備えたことを特徴とする中継装置。

【請求項 12】

ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在し、前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御装置に用いるサービス不能攻撃防御プログラムであって、

前記ネットワーク上に所在する正当な装置により送信された非攻撃バケットの送信元を示す正規アドレス情報を取得する正規アドレス情報取得手順と、

前記正規アドレス情報取得手順により取得された正規アドレス情報に基づいて非攻撃バケットの条件を示す正規条件情報を生成する正規条件情報生成手順と、

前記ネットワークから受信したバケットのうち前記正規条件情報生成手順により生成された正規条件情報に示された条件に適合するバケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうバケットの通過を制限するバケット制限手順と

をコンピュータに実行させることを特徴とするサービス不能攻撃防御プログラム。

【請求項 13】

前記正規アドレス情報取得手順は、前記中継装置に対して自装置のアドレス情報を通知するアドレス情報通知手順と、前記アドレス情報通知手順により通知した自装置のアドレス情報に応答して前記中継装置が返送した前記正当な装置からの正規アドレス情報を受信する受信手順とを含んだことを特徴とする請求項 12 に記載のサービス不能攻撃防御プログラム。

【請求項 14】

前記正規アドレス情報取得手順は、正規アドレス情報を一括管理する正規アドレス情報提供装置に対して前記正規アドレス情報の送信要求をおこなう正規アドレス情報送信要求手順と、前記正規アドレス情報の送信要求に応答して返送された正規アドレス情報を受信する受信手順とを含んだことを特徴とする請求項 12 に記載のサービス不能攻撃防御プログラム。

【請求項 15】

サービス不能攻撃対象となる通信機器に対するサービス不能攻撃を防御するゲート装置および／またはネットワークを形成する一または複数の中継装置と接続された中継装置に用いる中継装置用プログラムであって、

前記ゲート装置のアドレス情報を取得するアドレス情報取得手順と、

前記ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報を受信した際に、前記アドレス情報取得手順により取得されたアドレス情報に基づいて、前記ゲート装置または隣接する他の中継装置に前記正規アドレス情報を中継する正規アドレス情報中継手順と

をコンピュータに実行させることを特徴とする中継装置用プログラム。

【書類名】明細書

【発明の名称】 サービス不能攻撃防御方法、サービス不能攻撃防御装置、中継装置、サービス不能攻撃防御プログラムおよび中継装置用プログラム

【技術分野】

【0001】

この発明は、ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在するゲート装置若しくはこの中継装置で通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御方法、サービス不能攻撃防御装置、中継装置、サービス不能攻撃防御プログラムおよび中継装置用プログラムに関し、特に、防御対象の通信機器に対して攻撃をおこなわない非攻撃バケットの条件を表す正規条件情報を容易に管理することができるサービス不能攻撃防御方法、サービス不能攻撃防御装置、中継装置、サービス不能攻撃防御プログラムおよび中継装置用プログラムに関する。

【背景技術】

【0002】

従来、ネットワークを介した攻撃としてサービス不能攻撃および分散型サービス不能攻撃（Distributed Denial of Service Attack、以下単に「DDoS攻撃」と言う）が知られている。かかるDDoS攻撃から通信機器を防御する分散型サービス不能攻撃防御システムでは、攻撃対象となる通信機器とネットワークとの間に設けられたゲートウェイ装置やネットワークを構成するルータ装置がバケットを制限することになる。具体的には、ネットワークを介して通信機器に向けて送信されたバケットを正規バケット、容疑バケットまたは不正バケットに分類し、通信機器に送信されるバケットを制限していた（例えば、特許文献1参照）。

【0003】

このような従来の分散型サービス不能攻撃防御システムにおいては、あらかじめ登録された攻撃検知条件に基づいてゲートウェイ装置が攻撃を検知すると、攻撃検知されたバケットの特徴を示す容疑シグネチャが生成され、生成された容疑シグネチャがネットワークを構成するルータ装置等の中継装置に通知される。

【0004】

一方、容疑シグネチャに当てはまるバケットのうち通信機器に対する攻撃とみなされないバケット（以下「非攻撃バケット」と言う）の特徴を表す正規シグネチャが、あらかじめ登録された正規条件情報に基づいてゲートウェイ装置によって生成され、生成された正規シグネチャがネットワークを構成するルータ装置等の中継装置に通知される。

【0005】

容疑シグネチャおよび正規シグネチャが通知された中継装置並びにゲートウェイ装置によって中継されるバケットは、容疑シグネチャおよび正規シグネチャに基づいてシェーピングやフィルタリング等の処理が施される。

【0006】

このように、従来の分散型サービス不能攻撃防御システムは、攻撃を行うバケットの通過を出来るだけ攻撃元の近くで制限することによって、攻撃を行うバケット（以下「攻撃バケット」と言う）による悪影響を出来るだけ小さくするようになっている。

【0007】

【特許文献1】特開2003-283554号公報

【発明の開示】

【発明が解決しようとする課題】

【0008】

しかしながら、従来の分散型サービス不能攻撃防御システムにおいては、攻撃から防御する対象の通信機器に対する非攻撃バケットの条件を表す正規条件情報の追加や変更等の管理がゲートウェイ装置のオペレータによって行われるため、正規条件情報の管理が煩雑になるといった課題があった。

【0009】

本発明は、上述した従来技術による問題点を解消するためになされたものであり、防御対象の通信機器に対して攻撃をおこなわない非攻撃パケットの条件を表す正規条件情報を容易に管理することができるサービス不能攻撃防御方法、サービス不能攻撃防御装置、中継装置、サービス不能攻撃防御プログラムおよび中継装置用プログラムを提供することを目的とする。

【課題を解決するための手段】

【0010】

上述した課題を解決し、目的を達成するため、本発明は、ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在するゲート装置若しくは前記中継装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御方法であって、前記ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報を前記ゲート装置が取得する正規アドレス情報取得工程と、前記正規アドレス情報取得工程により取得された正規アドレス情報に基づいて前記ゲート装置が非攻撃パケットの条件を示す正規条件情報を生成する正規条件情報生成工程と、前記ゲート装置が前記ネットワークから受信したパケットのうち前記正規条件情報生成工程により生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうパケットの通過を制限するパケット制限工程とを含んだことを特徴とする。

【0011】

この発明によれば、ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報をゲート装置が取得し、取得した正規アドレス情報に基づいてゲート装置が非攻撃パケットの条件を示す正規条件情報を生成し、ゲート装置がネットワークから受信したパケットのうち生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、通信機器へ攻撃をおこなうパケットの通過を制限することとしたので、正規条件情報を効率良く生成することができる。

【0012】

また、本発明は、上記発明において、前記正規アドレス情報取得工程は、前記ゲート装置が前記中継装置に対して自装置のアドレス情報を通知するアドレス情報通知工程と、前記中継装置が前記正当な装置からの正規アドレス情報を受信した場合に、前記アドレス情報通知工程により通知された前記アドレス情報に基づいて当該正規アドレス情報を前記ゲート装置に対して中継する正規アドレス情報中継工程と、前記ゲート装置が前記正規アドレス情報を受信する受信工程とを含んだことを特徴とする。

【0013】

この発明によれば、ゲート装置が中継装置に対して自装置のアドレス情報を通知し、中継装置が正当な装置からの正規アドレス情報を受信した場合に、通知されたアドレス情報に基づいて当該正規アドレス情報をゲート装置に対して中継し、ゲート装置が正規アドレス情報を受信することとしたので、ゲート装置が中継装置に自装置のアドレス情報を通知するだけで、中継装置を介して正当な装置から送信された正規アドレス情報を入手することができる。

【0014】

また、本発明は、上記発明において、前記アドレス情報通知工程は、前記ゲート装置のアドレス情報を通知された中継装置が隣接する他の中継装置に前記ゲート装置のアドレス情報を中継し、前記正規アドレス情報中継工程は、前記他の中継装置が前記正当な装置からの正規アドレス情報を受信した場合に、前記ゲート装置のアドレス情報に基づいて隣接する中継装置若しくは前記ゲート装置に前記正規アドレス情報を中継することを特徴とする。

【0015】

この発明によれば、ゲート装置のアドレス情報を通知された中継装置が隣接する他の中継装置にゲート装置のアドレス情報を中継し、他の中継装置が正当な装置からの正規アドレス情報を受信した場合に、ゲート装置のアドレス情報に基づいて隣接する中継装置若し

くはゲート装置に前記正規アドレス情報を中継することとしたので、必要な各中継装置を経由しつつ効率良く正規アドレス情報をゲート装置まで中継することができる。

【0016】

また、本発明は、上記発明において、前記正規アドレス情報取得工程は、正規アドレス情報を一括管理する正規アドレス情報提供装置が前記正規アドレス情報を各正当な装置から受信して格納する正規アドレス情報格納工程と、前記正規アドレス情報提供装置が前記ゲート装置から前記正規アドレス情報の送信要求を受け付けた場合に、送信要求された正規アドレス情報を前記ゲート装置に対して通知する正規アドレス情報通知工程と、前記ゲート装置が前記正規アドレス情報を受信する受信工程とを含んだことを特徴とする。

【0017】

この発明によれば、正規アドレス情報を一括管理する正規アドレス情報提供装置が正規アドレス情報を各正当な装置から受信して格納しておき、この正規アドレス情報提供装置がゲート装置から正規アドレス情報の送信要求を受け付けた場合に、送信要求された正規アドレス情報をゲート装置に対して通知し、ゲート装置が正規アドレス情報を受信することとしたので、ゲート装置が自装置のアドレス情報を事前に通知しなくても、必要の都度正規アドレス情報提供装置から正規アドレス情報を取得することができる。

【0018】

また、本発明は、上記発明において、前記正規アドレス情報取得工程は、アドレスを発行するアドレス発行装置若しくは正当な認証を受けた通信機器を前記ネットワーク上に所在する正当な装置により送信された前記正規アドレス情報を前記ゲート装置が取得することを特徴とする。

【0019】

この発明によれば、アドレスを発行するアドレス発行装置若しくは正当な認証を受けた通信機器をネットワーク上に所在する正当な装置とみなして、これらから送信された正規アドレス情報をゲート装置が取得することとしたので、正当な装置から受信した正しい正規アドレス情報に基づく正規条件情報を生成でき、不正な攻撃を看過する事態を防ぐことができる。

【0020】

また、本発明は、上記発明において、前記ゲート装置が前記ネットワークから受信されたバケットによる攻撃を検知する攻撃検知工程と、前記攻撃検知工程により攻撃が検知されたバケットの特徴を表す容疑シグネチャを生成する容疑シグネチャ生成工程と、前記正規条件情報生成工程により生成された正規条件情報を正規条件情報記憶部に格納する正規条件情報格納工程と、前記容疑シグネチャ生成工程により生成された容疑シグネチャに該当するバケットのうち、前記正規条件情報に示された条件に適合するバケットの特徴を表す正規シグネチャを生成する正規シグネチャ生成工程とをさらに含み、前記バケット制限工程は、前記容疑シグネチャ生成工程により生成された容疑シグネチャおよび前記正規シグネチャ生成工程により生成された正規シグネチャに基づいて前記ネットワークから受信したバケットの通過を制限することを特徴とする。

【0021】

この発明によれば、ゲート装置がネットワークから受信されたバケットによる攻撃を検知し、攻撃が検知されたバケットの特徴を表す容疑シグネチャを生成し、正規条件情報を正規条件情報記憶部に格納し、容疑シグネチャに該当するバケットのうち正規条件情報に示された条件に適合するバケットの特徴を表す正規シグネチャを生成し、生成された容疑シグネチャおよび正規シグネチャに基づいてネットワークから受信したバケットの通過を制限することとしたので、容疑シグネチャおよび正規シグネチャという従来の指標を利用しつつ効率良く攻撃バケットの通過を制限することができる。

【0022】

また、本発明は、上記発明において、前記容疑シグネチャ生成工程により生成された容疑シグネチャおよび前記正規シグネチャ生成工程により生成された正規シグネチャを前記ゲート装置が前記中継装置に通知するシグネチャ通知工程と、前記中継装置が前記シグネ

チャ通知工程により通知された容疑シグネチャおよび正規シグネチャに基づいてパケットの通過を制限制御するパケット制限制御工程とをさらに含んだことを特徴とする。

【0023】

この発明によれば、容疑シグネチャおよび正規シグネチャをゲート装置が中継装置に通知し、通知された容疑シグネチャおよび正規シグネチャに基づいて中継装置がパケットの通過を制限制御することとしたので、中継装置においても効率良く攻撃パケットの通過を制限することができる。

【0024】

また、本発明は、ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在し、前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御装置であって、前記ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報を取得する正規アドレス情報取得手段と、前記正規アドレス情報取得手段により取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成する正規条件情報生成手段と、前記ネットワークから受信したパケットのうち前記正規条件情報生成手段により生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうパケットの通過を制限するパケット制限手段とを備えたことを特徴とする。

【0025】

この発明によれば、ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報を取得し、取得した正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成し、ネットワークから受信したパケットのうち生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、通信機器へ攻撃をおこなうパケットの通過を制限することとしたので、正規条件情報を効率良く生成することができる。

【0026】

また、本発明は、上記発明において、前記正規アドレス情報取得手段は、前記中継装置に対して自装置のアドレス情報を通知するアドレス情報通知手段と、前記アドレス情報通知手段により通知した自装置のアドレス情報に応答して前記中継装置が返送した前記正当な装置からの正規アドレス情報を受信する受信手段とを備えたことを特徴とする。

【0027】

この発明によれば、中継装置に対して自装置のアドレス情報を通知し、通知した自装置のアドレス情報に応答して中継装置が返送した正当な装置からの正規アドレス情報を受信することとしたので、ゲート装置が中継装置に自装置のアドレス情報を通知するだけで、中継装置を介して正当な装置から送信された正規アドレス情報を入手することができる。

【0028】

また、本発明は、上記発明において、前記正規アドレス情報取得手段は、正規アドレス情報を一括管理する正規アドレス情報提供装置に対して前記正規アドレス情報の送信要求をおこなう正規アドレス情報送信要求手段と、前記正規アドレス情報の送信要求に応答して返送された正規アドレス情報を受信する受信手段とを備えたことを特徴とする。

【0029】

この発明によれば、正規アドレス情報を一括管理する正規アドレス情報提供装置に対して正規アドレス情報の送信要求をおこない、この正規アドレス情報の送信要求に応答して返送された正規アドレス情報を受信することとしたので、ゲート装置が自装置のアドレス情報を事前に通知しなくても、必要の都度正規アドレス情報提供装置から正規アドレス情報を取得することができる。

【0030】

また、本発明は、サービス不能攻撃対象となる通信機器に対するサービス不能攻撃を防御するゲート装置および／またはネットワークを形成する一または複数の中継装置と接続された中継装置であって、前記ゲート装置のアドレス情報を取得するアドレス情報取得手段と、前記ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信

元を示す正規アドレス情報を受信した際に、前記アドレス情報取得手段により取得されたアドレス情報に基づいて、前記ゲート装置または隣接する他の中継装置に前記正規アドレス情報を中継する正規アドレス情報中継手段とを備えたことを特徴とする。

【0031】

この発明によれば、ゲート装置のアドレス情報を取得しておき、ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報を受信した際に、取得されたアドレス情報に基づいて、ゲート装置または隣接する他の中継装置に正規アドレス情報を中継することとしたので、効率良く正規アドレス情報をゲート装置まで中継することができる。

【0032】

また、本発明は、ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在し、前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御装置に用いるサービス不能攻撃防御プログラムであって、前記ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報を取得する正規アドレス情報取得手順と、前記正規アドレス情報取得手順により取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成する正規条件情報生成手順と、前記ネットワークから受信したパケットのうち前記正規条件情報生成手順により生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうパケットの通過を制限するパケット制限手順とをコンピュータに実行させることを特徴とする。

【0033】

この発明によれば、ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報を取得し、取得した正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成し、ネットワークから受信したパケットのうち生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、通信機器へ攻撃をおこなうパケットの通過を制限することとしたので、正規条件情報を効率良く生成することができる。

【0034】

また、本発明は、上記発明において、前記正規アドレス情報取得手順は、前記中継装置に対して自装置のアドレス情報を通知するアドレス情報通知手順と、前記アドレス情報通知手順により通知した自装置のアドレス情報に応答して前記中継装置が返送した前記正当な装置からの正規アドレス情報を受信する受信手順とを含んだことを特徴とする。

【0035】

この発明によれば、中継装置に対して自装置のアドレス情報を通知し、通知した自装置のアドレス情報に応答して中継装置が返送した正当な装置からの正規アドレス情報を受信することとしたので、ゲート装置が中継装置に自装置のアドレス情報を通知するだけで、中継装置を介して正当な装置から送信された正規アドレス情報を入手することができる。

【0036】

また、本発明は、上記発明において、前記正規アドレス情報取得手順は、正規アドレス情報を一括管理する正規アドレス情報提供装置に対して前記正規アドレス情報の送信要求をおこなう正規アドレス情報送信要求手順と、前記正規アドレス情報の送信要求に応答して返送された正規アドレス情報を受信する受信手順とを含んだことを特徴とする。

【0037】

この発明によれば、正規アドレス情報を一括管理する正規アドレス情報提供装置に対して正規アドレス情報の送信要求をおこない、この正規アドレス情報の送信要求に応答して返送された正規アドレス情報を受信することとしたので、ゲート装置が自装置のアドレス情報を事前に通知しなくても、必要の都度正規アドレス情報提供装置から正規アドレス情報を取得することができる。

【0038】

また、本発明は、サービス不能攻撃対象となる通信機器に対するサービス不能攻撃を防

御するゲート装置および／またはネットワークを形成する一または複数の中継装置と接続された中継装置に用いる中継装置用プログラムであって、前記ゲート装置のアドレス情報を取得するアドレス情報取得手順と、前記ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報を受信した際に、前記アドレス情報取得手順により取得されたアドレス情報に基づいて、前記ゲート装置または隣接する他の中継装置に前記正規アドレス情報を中継する正規アドレス情報中継手順とをコンピュータに実行させることを特徴とする。

【0039】

この発明によれば、ゲート装置のアドレス情報を取得しておき、ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報を受信した際に、取得されたアドレス情報に基づいて、ゲート装置または隣接する他の中継装置に正規アドレス情報を中継することとしたので、効率良く正規アドレス情報をゲート装置まで中継することができる。

【発明の効果】

【0040】

本発明によれば、ネットワーク上に所在する正当な装置により送信された非攻撃パケットの送信元を示す正規アドレス情報をゲート装置が取得し、取得した正規アドレス情報に基づいてゲート装置が非攻撃パケットの条件を示す正規条件情報を生成し、ゲート装置がネットワークから受信したパケットのうち生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、通信機器へ攻撃をおこなうパケットの通過を制限するよう構成したので、正規条件情報を効率良く生成することができ、もってゲート装置のオペレータによる正規条件情報の管理負担を軽減することができる。

【0041】

また、本発明によれば、ゲート装置が中継装置に対して自装置のアドレス情報を通知し、中継装置が正当な装置からの正規アドレス情報を受信した場合に、通知されたアドレス情報に基づいて当該正規アドレス情報をゲート装置に対して中継し、ゲート装置が正規アドレス情報を受信するよう構成したので、ゲート装置が中継装置に自装置のアドレス情報を通知するだけで、中継装置を介して正当な装置から送信された正規アドレス情報を入手することができる。

【0042】

また、本発明によれば、ゲート装置のアドレス情報を通知された中継装置が隣接する他の中継装置にゲート装置のアドレス情報を中継し、他の中継装置が正当な装置からの正規アドレス情報を受信した場合に、ゲート装置のアドレス情報に基づいて隣接する中継装置若しくはゲート装置に前記正規アドレス情報を中継するよう構成したので、必要な各中継装置を経由しつつ効率良く正規アドレス情報をゲート装置まで中継することができる。

【0043】

また、本発明によれば、正規アドレス情報を一括管理する正規アドレス情報提供装置が正規アドレス情報を各正当な装置から受信して格納しておき、この正規アドレス情報提供装置がゲート装置から正規アドレス情報の送信要求を受け付けた場合に、送信要求された正規アドレス情報をゲート装置に対して通知し、ゲート装置が正規アドレス情報を受信するよう構成したので、ゲート装置が自装置のアドレス情報を事前に通知しなくても、必要の都度正規アドレス情報提供装置から正規アドレス情報を取得することができる。

【0044】

また、本発明によれば、アドレスを発行するアドレス発行装置若しくは正当な認証を受けた通信機器をネットワーク上に所在する正当な装置とみなして、これらから送信された正規アドレス情報をゲート装置が取得するよう構成したので、正当な装置から受信した正しい正規アドレス情報に基づく正規条件情報を生成でき、不正な攻撃を看過する事態を防ぐことができる。

【0045】

また、本発明によれば、ゲート装置がネットワークから受信されたパケットによる攻撃

を検知し、攻撃が検知されたバケットの特徴を表す容疑シグネチャを生成し、正規条件情報を正規条件情報記憶部に格納し、容疑シグネチャに該当するバケットのうち正規条件情報に示された条件に適合するバケットの特徴を表す正規シグネチャを生成し、生成された容疑シグネチャおよび正規シグネチャに基づいてネットワークから受信したバケットの通過を制限するよう構成したので、容疑シグネチャおよび正規シグネチャという従来の指標を利用しつつ効率良く攻撃バケットの通過を制限することができる。

【0046】

また、本発明によれば、容疑シグネチャおよび正規シグネチャをゲート装置が中継装置に通知し、通知された容疑シグネチャおよび正規シグネチャに基づいて中継装置がバケットの通過を制限制御するよう構成したので、中継装置においても効率良く攻撃バケットの通過を制限することができる。

【0047】

また、本発明によれば、ゲート装置のアドレス情報を取得しておき、ネットワーク上に所在する正当な装置により送信された非攻撃バケットの送信元を示す正規アドレス情報を受信した際に、取得されたアドレス情報に基づいて、ゲート装置または隣接する他の中継装置に正規アドレス情報を通知するよう構成したので、効率良く正規アドレス情報をゲート装置まで通知することができる。

【発明を実施するための最良の形態】

【0048】

以下に添付図面を参照して、この発明に係るサービス不能攻撃防御方法、サービス不能攻撃防御装置中継装置、サービス不能攻撃防御プログラムおよび中継装置用プログラムの好適な実施の形態を詳細に説明する。なお、下記に示す実施例1では、アドレス発行サーバ装置から中継装置に対して正規アドレス情報の送信要求をおこなう場合を示し、実施例2では正規アドレス情報を一括管理する正規アドレス情報提供サーバへゲート装置から正規アドレス情報の送信要求をおこなう場合を示すこととする。

【実施例1】

【0049】

図1は、本実施例1に係る分散型サービス不能攻撃防御システム1の構成を示すブロック図である。同図に示す分散型サービス不能攻撃防御システム1は、通信機器7への分散型サービス不能攻撃を主としてゲート装置8で防御するシステムである。具体的には、ネットワーク2上に所在する正当な装置（アドレス発行サーバ10）により送信された非攻撃バケットの送信元を示す正規アドレス情報をゲート装置8が取得し、取得した正規アドレス情報に基づいてゲート装置8が非攻撃バケットの条件を示す正規条件情報を生成し、ネットワークから受信したバケットのうち正規条件情報に示された条件に適合するバケットの通過を許容しつつ、通信機器7へ攻撃をおこなうバケットの通過を制限するようにしている。なお、このゲート装置8が正規条件情報に基づいて生成した正規シグネチャ並びに容疑シグネチャは中継装置6などに中継され、中継装置でのフィルタリングを可能ならしめている。

【0050】

従来、かかる正規アドレス情報の追加や変更等の管理は、ゲート装置8のオペレータによって行われていたため、正規条件情報の管理が煩雑になるという問題があった。このため、本実施例では、かかる正規アドレス情報の追加をゲート装置8のオペレータに担わせるのではなく、アドレス発行サーバ10などの正当な端末から正規アドレス情報を取得することとしている。このため、本実施例1によれば、ゲート装置8のオペレータの管理負担を軽減することができる。

【0051】

ここで、このゲート装置8が正規アドレス情報を取得する際に、本実施例1では、ゲート装置8が中継装置6に対して自装置のアドレス情報を通知し（図1のステップ1）、この中継装置6にアドレス情報を記憶させ（図1のステップ2）、アドレス発行サーバ10から発行された正規アドレス情報送信要求（正規アドレス情報を含む）を中継装置6が受

信すると、あらかじめ記憶したアドレス情報に基づいてゲート装置 8 に中継し（図 1 のステップ 3）、ゲート装置 8 が受信した正規アドレス情報に基づいて正規条件情報を自動生成する（図 1 のステップ 4）こととしている。

【0052】

次に、この分散型サービス不能攻撃防御システム 1 のシステム構成について説明する。図 1 に示すように、この分散型サービス不能攻撃防御システム 1 は、ネットワーク 2 を介して伝送されるパケットを中継する複数の中継装置 3～6 と、ネットワーク 2 を介して通信機器 7 に送信されるパケットの通過を制限するゲート装置 8 とを備えている。なお、図 1 に示した分散型サービス不能攻撃防御システム 1 の構成は一例を示すものであり、中継装置およびゲート装置等の数量やネットワーク構成を限定するものではない。

【0053】

ゲート装置 8 は、ネットワーク間接続機器であるゲートウェイ装置などによって構成され、コンピュータ装置等によって構成される通信機器 7 を含む構内情報通信網（Local Area Network、以下単に「LAN」と記載する。）14 に接続されている。また、中継装置 3～6 は、ルータ装置によってそれぞれ構成されている。なお、この中継装置 3～6 は、ブリッジによって構成することもできる。

【0054】

ここで、中継装置 3 は、中継装置 4 およびゲート装置 8 に接続され、中継装置 4 は、通信機器 15 および中継装置 3 に接続され、中継装置 5 は、通信機器 16 および中継装置 6 に接続され、中継装置 6 は、中継装置 5、エッジルータ 11 およびゲート装置 8 に接続されている。

【0055】

図 2 は、図 1 に示したゲート装置 8 の構成を示すブロック図である。図 2 に示すように、このゲート装置 8 は、ネットワーク 2 から受信されたパケットによる攻撃を検知する攻撃検知部 20 と、攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成する容疑シグネチャ生成部 21 と、通信機器 7 に対する攻撃とみなされないパケット（非攻撃パケット）の条件を表す正規条件情報を格納する正規条件情報格納部 22 と、正規条件情報格納部 22 に格納される正規条件情報を生成する正規条件情報生成部 23 と、容疑シグネチャに当てはまるパケットのうち、正規条件情報に表された条件に合うパケットの特徴を表す正規シグネチャを生成する正規シグネチャ生成部 24 と、容疑シグネチャに当てはまるパケットのうち、通信機器 7 に対する攻撃とみなすパケットの特徴を表す不正シグネチャを生成する不正シグネチャ生成部 25 と、容疑シグネチャ、正規シグネチャおよび不正シグネチャに基づいてネットワーク 2 から受信されたパケットの通過を制限するパケット制限部 26 と、容疑シグネチャおよび正規シグネチャを隣接関係にある中継装置 3 および中継装置 6 に通知するシグネチャ通知部 27 と、ネットワーク 2 に接続された各装置と通信を行うネットワークインタフェース 28 とを備えている。

【0056】

攻撃検知部 20 は、あらかじめ設定された攻撃検知条件に基づいて攻撃を検知する処理部である。図 3 は、攻撃検知条件の一例を示す図である。図 3 において、攻撃検知条件は、検知属性、検知閾値および検知時間の組からなる 3 組のレコードで構成される。検知属性は、検知対象とするパケットの属性を示し、検知閾値は、検知対象となるパケットの伝送レートの閾値を示し、検知時間は、検知対象となるパケットの伝送レートが検知閾値を超える時間の閾値を示している。

【0057】

例えば、1 番目の検知条件は、宛先のアドレス情報が 192.168.1.1 であり（Dst=192.168.1.1/32）、トランスポート層のプロトコルが TCP（Transmission Control Protocol）であり（Protocol=TCP）、TCP ポート番号が 80 である（Port=80）パケットが検知対象となり、この検知対象のパケットの伝送レートが 500 kbps を超えた状態が 10 秒以上続いた場合には、検知対象のパケットによる攻撃として検知される。

【0058】

同様に、2番目の検知条件は、宛先のアドレス情報が192.168.1.2であり（Dst=192.168.1.2/32）、トランスポート層のプロトコルがUDP（User datagram protocol）である（Protocol=UDP）パケットが検知対象となり、この検知対象のパケットの伝送レートが300 kbpsを超えた状態が10秒以上続いた場合には、検知対象のパケットによる攻撃として検知される。

【0059】

また、3番目の検知条件は、宛先のアドレス情報が192.168.1.0～192.168.1.255の範囲内である（Dst=192.168.1.0/24）パケットが検知対象となり、この検知対象のパケットの伝送レートが1 Mbpsを超えた状態が20秒以上続いた場合には、検知対象のパケットによる攻撃として検知される。

【0060】

このように、検知対象のパケットによる攻撃が攻撃検知部20によって検知されると、容疑シグネチャ生成部21は、検知対象のパケットの特徴を表す容疑シグネチャを生成する。例えば、図3における攻撃検知条件の1番目の検知条件に合う攻撃が検知された場合には、容疑シグネチャ生成部21は、宛先のアドレス情報が192.168.1.1であり、トランスポート層のプロトコルがTCPであり、TCPポート番号が80であるパケットを示す容疑シグネチャを生成する。なお、容疑シグネチャは、対象となるパケットに対するシェーピングやフィルタリング等の処理や、この処理に関するパラメータ等を含むようにしてもよい。

【0061】

正規条件情報格納部22は、フラッシュメモリなどの不揮発性の記憶媒体によって構成されている。図4は、正規条件情報格納部22に格納される正規条件情報の一例を示す図である。図4において、正規条件情報は攻撃とみなされない条件である正規条件で構成される。

【0062】

例えば、1番目の正規条件によって、送信元のアドレス情報が172.16.10.0～172.16.10.255の範囲内である（Src=172.16.10.0/24）パケットは、攻撃とみなされない。同様に、2番目の正規条件によって、サービスタイプ（Type of Service）が0x01である（TOS=0x01）パケットは、攻撃とみなされない。

【0063】

正規条件情報生成部23は、本実施例の最も重要な特徴部分をなす処理部であり、オペレータの処理行為を伴うことなく正規条件情報格納部22に格納された正規条件情報の自動更新をおこなう。従来、かかる正規条件情報の管理はオペレータに委ねられていたが、本実施例では、かかる正規条件情報を自動更新している。

【0064】

具体的には、この正規条件情報生成部23は、ネットワーク2を介した攻撃を行わないパケットの送信元を表す正規アドレス情報が何れかの中継装置3～6から送信され、送信された正規アドレス情報がネットワークインタフェース28に受信された場合に、正規アドレス情報に基づいて正規条件情報を生成し、生成した正規条件情報を以って正規条件情報格納部22に格納された正規条件情報を更新する。すなわち、正規アドレス情報を送信アドレスとしたパケットは、通信機器7に対する攻撃とみなされないものとなる。なお、ここでは正規条件情報の追加を自動的におこなう点を強調したが、正規条件情報格納部22に格納された正規条件情報は、ゲート装置8のオペレータによって追加、削除、変更などの編集ができるようにしてもよい。

【0065】

正規シグネチャ生成部24は、容疑シグネチャ生成部21によって生成された容疑シグネチャに当てはまるパケットのうち、正規条件情報に表された条件に合うパケットの特徴を表す正規シグネチャを生成する処理部である。

【0066】

例えば、この正規シグネチャ生成部24は、攻撃検知部20によって図3に示した1番

目の攻撃検知条件に合う攻撃が検知された場合には、図4に示した正規条件情報に基づいて、宛先のアドレス情報が192.168.1.1であり、トランスポート層のプロトコルがTCPであり、TCPポート番号が80であり、送信元のアドレス情報が172.16.10.0~172.16.10.255の範囲内であるパケットを示す正規シグネチャと、宛先のアドレス情報が192.168.1.1であり、トランスポート層のプロトコルがTCPであり、TCPポート番号が80であり、サービスタイプが0x01であるパケットを示す正規シグネチャとを生成する。

【0067】

不正シグネチャ生成部25は、容疑シグネチャ生成部21によって生成された容疑シグネチャに当てはまるパケットのうち、不正条件に合うパケットの特徴を表す不正シグネチャを生成する処理部である。

【0068】

図5は、不正条件の一例を示す図である。図5において、1番目の不正条件は、500kbps以上の伝送レートで30秒以上連続送信されているパケットを示している。同様に、2番目の不正条件は、300kbps以上の伝送レートで15秒以上連続送信されているICMP(Internet Control Message Protocol)に準拠したエコー応答(Echo Reply)パケットを示し、3番目の不正条件は、300kbps以上の伝送レートで15秒以上連続送信されている分割送信されたフラグメントパケットを示している。

【0069】

パケット制限部26は、容疑シグネチャ生成部21によって生成された容疑シグネチャと正規シグネチャ生成部24によって生成された正規シグネチャと不正シグネチャ生成部25によって生成された不正シグネチャに基づいてネットワークインタフェース28によって受信されたパケットの通過を制限するようになっている。

【0070】

具体的には、パケット制限部26は、不正シグネチャに当てはまるパケットを廃棄し、正規シグネチャに当てはまるパケットに対しては制限を加えずに通過させ、容疑シグネチャに当てはまるパケットに対しては容疑シグネチャに示された処理等に基づいて伝送帯域を絞った経路を介して通過させるようになっている。

【0071】

シグネチャ通知部27は、容疑シグネチャおよび正規シグネチャを隣接関係にある中継装置3および中継装置6に通知する処理部であり、中継装置3および中継装置6は、さらに隣接関係にある中継装置にパケットを中継する。なお、隣接関係とは、本発明に係るゲート装置および中継装置における隣接関係であり、物理的な接続関係とは異なる。

【0072】

また、シグネチャ通知部27は、ゲート装置8のアドレス情報を容疑シグネチャおよび正規シグネチャと同様に隣接関係にある中継装置3および中継装置6に通知し、中継装置3および中継装置6は、さらに隣接関係にある中継装置にゲート装置8のアドレス情報を中継する。なお、シグネチャ通知部27によるゲート装置8のアドレス情報の通知は、ゲート装置8のオペレータによる起動に応じて行なうことができ、定期的に行われるようにしてもよい。

【0073】

図6は、図1に示した中継装置6の構成を示す機能ブロック図である。なお、ここでは説明の便宜上中継装置6の構成を説明するが、他の中継装置3~5についても中継装置6と同様に構成されている。この中継装置6は、入力ポート30と、パケットをルーティングするためのスイッチ31と、出力ポート32と、不正シグネチャを生成する不正シグネチャ生成部35と、不正シグネチャならびにゲート装置8によって通知された容疑シグネチャおよび正規シグネチャに基づいて入力ポート30に入力されたパケットの通過を制限するパケット制限部36と、容疑シグネチャおよび正規シグネチャを隣接関係にある中継装置5に中継するシグネチャ中継部37と、ゲート装置8のアドレス情報を記憶するアドレス情報記憶部38と、アドレス情報記憶部38に記憶されたゲート装置8のアドレス情報に基づいて正規アドレス情報を送信する正規アドレス情報送信部39とを備えている。

【0074】

ここで、不正シグネチャ生成部35、バケット制限部36およびシグネチャ中継部37は、ゲート装置8を構成する不正シグネチャ生成部25、バケット制限部26およびシグネチャ通知部27とそれぞれ同様に構成されるため、詳細な説明は省略する。なお、中継装置6は、ゲート装置8と同様に、攻撃検知部、容疑シグネチャ生成部、正規条件情報格納部および正規シグネチャ生成部を備えるようにしてもよい。

【0075】

シグネチャ中継部37は、バケット制限部36によってバケットの通過が制限された後、制限された伝送レートを超えた容疑シグネチャに当てはまるバケットが入力ポート30に受信されているか否かを判断し、制限された伝送レートを超えた容疑シグネチャに当てはまるバケットが入力ポート30に受信されていると判断した場合には、容疑シグネチャおよび正規シグネチャを中継し、制限された伝送レートを超えた容疑シグネチャに当てはまるバケットが入力ポート30に受信されていると判断しなかった場合には、容疑シグネチャおよび正規シグネチャを中継しない。

【0076】

また、図1に示した構成においては、中継装置4および中継装置5には、容疑シグネチャおよび正規シグネチャを中継する中継装置が存在しないため、シグネチャ中継部37による容疑シグネチャおよび正規シグネチャの中継は行われない。

【0077】

このように、ゲート装置8によって攻撃が検知された場合には、容疑シグネチャおよび正規シグネチャが生成され、生成された容疑シグネチャおよび正規シグネチャが各中継装置3～6に通知され、ゲート装置8および中継装置3～6においてバケットのシェーピングやフィルタリング等の処理が施される。このため、分散型サービス不能攻撃防御システム1においては、例えば、ゲート装置8によって検知された攻撃が通信機器15を介して行われている場合には、攻撃を行うバケットの通過が攻撃元の近く、すなわち中継装置4で制限され、攻撃を行うバケットによる悪影響が小さくなる。

【0078】

アドレス情報記憶部38は、不揮発性の記憶媒体によって構成されており、ゲート装置8のシグネチャ通知部27や各中継装置のシグネチャ中継部37を介して通知および中継されたゲート装置8のアドレス情報を記憶する。なお、図1においては、一つゲート装置8を図示しているが、本実施例の分散型サービス不能攻撃防御システム1は、複数のゲート装置によって構成することもでき、この場合にアドレス情報記憶部38には、各ゲート装置のアドレス情報が記憶されることになる。

【0079】

図1において、LAN9は、エッジルータ11を介してネットワーク2と接続されるとともに、コンピュータ装置等の通信機器12、13が接続されている。ここで、LAN9では、ネットワーク2を介した攻撃を行わないものとする。

【0080】

LAN9に接続されたアドレス発行サーバ10は、LAN9のアドレス情報またはLAN9に接続された通信機器12、13のアドレス情報を含む正規アドレス情報送信要求を中継装置6に向けて送信する。なお、このアドレス発行サーバ10は、正規アドレス情報送信要求を定期的に送信するようにしてもよく、アドレス発行サーバ10のオペレータによる起動に応じて送信するようにしてもよい。また、正規アドレス情報送信要求を送信するものとしては、アドレス発行サーバ10の他にエッジルータ11等のLAN9を構成する装置であれば何れのものでもよい。

【0081】

図6において、正規アドレス情報送信部39は、アドレス発行サーバ10によって送信された正規アドレス情報送信要求に回答して、正規アドレス情報送信要求に含まれるアドレス情報、すなわち正規アドレス情報をアドレス情報記憶部38に記憶された各ゲート装置のアドレス情報に基づいて送信する。

【0082】

以上のように構成された分散型サービス不能攻撃防御システム1について、図7～図10を用いてその動作を説明する。図7は、図1に示したゲート装置8の攻撃検知動作を示すフローチャートである。

【0083】

まず、攻撃検知条件に基づいてネットワークインタフェース28によって受信されたパケットによる攻撃が攻撃検知部20によって検知されると（ステップS1）、攻撃が検知されたパケットの特徴を表す容疑シグネチャが容疑シグネチャ生成部21によって生成される（ステップS2）。

【0084】

次に、容疑シグネチャに当てはまるパケットのうち、正規条件情報に表された条件に合うパケットの特徴を表す正規シグネチャが正規シグネチャ生成部24によって生成されるとともに（ステップS3）、容疑シグネチャに当てはまるパケットのうち、不正条件に合うパケットの特徴を表す不正シグネチャが不正シグネチャ生成部25によって生成される（ステップS4）。

【0085】

次に、容疑シグネチャ、正規シグネチャおよび不正シグネチャがパケット制限部26によるパケット通過条件として設定される（ステップS5）。また、容疑シグネチャおよび正規シグネチャがシグネチャ通知部27によって隣接関係にある中継装置3および中継装置6に通知される（ステップS6）。

【0086】

図8は、図1に示した中継装置6のシグネチャ受信動作を示すフローチャートである。まず、入力ポート30に容疑シグネチャおよび正規シグネチャが受信されると（ステップS10）、受信された容疑シグネチャに当てはまるパケットのうち、不正条件に合うパケットの特徴を表す不正シグネチャが不正シグネチャ生成部35によって生成される（ステップS11）。

【0087】

次に、容疑シグネチャ、正規シグネチャおよび不正シグネチャがパケット制限部36によるパケット通過条件として設定される（ステップS12）。また、容疑シグネチャおよび正規シグネチャがシグネチャ中継部37によって隣接関係にある中継装置5に通知される（ステップS13）。

【0088】

図9は、図1に示したゲート装置8のパケット制限動作を示すフローチャートである。まず、ネットワークインタフェース28にパケットが受信されると（ステップS20）、受信されたパケットが不正シグネチャに当てはまるか否かがパケット制限部26によって判断される（ステップS21）。

【0089】

パケットが不正シグネチャに当てはまると判断された場合には、パケットがパケット制限部26によって廃棄される（ステップS22）。一方、パケットが不正シグネチャに当てはまらないと判断された場合には、パケットが正規シグネチャに当てはまるか否かがパケット制限部26によって判断される（ステップS23）。

【0090】

パケットが正規シグネチャに当てはまると判断された場合には、パケットの通過がパケット制限部26によって許可される（ステップS24）。一方、パケットが正規シグネチャに当てはまらないと判断された場合には、パケットが容疑シグネチャに当てはまるか否かがパケット制限部26によって判断される（ステップS25）。

【0091】

パケットが容疑シグネチャに当てはまると判断された場合には、容疑シグネチャに示された処理等に基づいて伝送帯域が絞られた経路を介したパケットの通過が許可される（ステップS26）。一方、パケットが容疑シグネチャに当てはまらないと判断された場合に

は、バケットの通過がバケット制限部 26 によって許可される（ステップ S 24）。なお、中継装置 3～6 のバケット制限動作は、ゲート装置 8 のバケット制限動作と同様であるため説明を省略する。

【0092】

図 10 は、分散型サービス不能攻撃防御システム 1 の正規条件情報更新動作を示すシーケンス図である。まず、ゲート装置 8 のアドレス情報が、ゲート装置 8 のシグネチャ通知部 27 によって中継装置 3 および中継装置 6 にそれぞれ通知される（ステップ S 30、S 31）。中継装置 3 に通知されたゲート装置 8 のアドレス情報は、中継装置 3 のシグネチャ中継部 37 によって中継装置 4 に中継される（ステップ S 32）。

【0093】

中継装置 6 に通知されたゲート装置 8 のアドレス情報は、中継装置 6 のシグネチャ中継部 37 によって中継装置 5 に中継されるとともに（ステップ S 33）、アドレス情報記憶部 38 に記憶される（ステップ S 34）。なお、中継装置 3～5 においてもアドレス情報記憶部 38 にゲート装置 8 のアドレス情報が記憶されるがここでは図示省略する。

【0094】

ここで、LAN 9 のアドレス発行サーバ 10 によって正規アドレス情報送信要求が中継装置 6 に送信されると（ステップ S 35）、中継装置 6 のアドレス情報記憶部 38 に記憶されたゲート装置 8 のアドレス情報に基づいて正規アドレス情報送信要求に含まれる正規アドレス情報が送信される（ステップ S 36）。

【0095】

正規アドレス情報がゲート装置 8 のネットワークインタフェース 28 に受信されると、受信された正規アドレス情報に基づいて正規条件情報が正規条件情報生成部 23 によって生成され（ステップ S 37）、生成された正規条件情報を以て正規条件情報格納部 22 に格納された正規条件情報が更新される（ステップ S 38）。

【0096】

以上説明したように、分散型サービス不能攻撃防御システム 1 によれば、ネットワーク 2 を介した攻撃を行わないバケットの送信元を表す正規アドレス情報がゲート装置 8 に送信され、ゲート装置 8 に送信された正規アドレス情報に基づいて、通信機器 7 に対する攻撃とみなされないバケットの条件を表す正規条件情報を更新するため、正規条件情報を容易に管理することができる。

【実施例 2】

【0097】

ところで、上記実施例 1 では、ゲート装置 8 が正規アドレス情報を取得する際に、本実施例 1 では、ゲート装置 8 のアドレス情報を中継装置 6 で記憶しておき、この中継装置 6 がアドレス発行サーバ 10 から発行された正規アドレス情報送信要求（正規アドレス情報を含む）を受信すると、あらかじめ記憶したアドレス情報に基づいてゲート装置 8 に中継することにより、ゲート装置 8 が正規アドレス情報を取得することとしたが、本発明はこれに限定されるものではない。そこで、本実施例 2 では、正規アドレス情報を一括管理する正規アドレス情報提供サーバを設け、この正規アドレス情報提供サーバへの要求に応答してゲート装置が正規アドレス情報を取得する場合を説明する。

【0098】

図 11 は、本発明の実施例 2 に係る分散型サービス不能攻撃防御システム 50 の構成を示すブロック図である。なお、分散型サービス不能攻撃防御システム 50 の各構成において実施例 1 に係る分散型サービス不能攻撃防御システム 1 の各構成と同様なものについては同一の符号を付して説明を省略する。

【0099】

同図に示す分散型サービス不能攻撃防御システム 50 は、正規アドレス情報を一括管理する正規アドレス情報提供サーバ 59 からゲート装置 58 に対して正規アドレス情報を提供している。具体的には、アドレス発行サーバ 60 があらかじめ正規アドレス情報提供サーバ 59 に正規アドレス情報を通知し（図 11 のステップ 1）、この正規アドレス情報提

供サーバ59に正規アドレス情報を記憶しておく（図11のステップ2）。そして、ゲート装置58から正規アドレス情報提供サーバ59に正規アドレス情報送信要求がなされると（図11のステップ3）、この正規アドレス情報提供サーバ59がゲート装置58に正規アドレス情報を送信し（図11のステップ4）、ゲート装置58が受信した正規アドレス情報に基づいて正規条件情報を自動生成する（図11のステップ5）こととしている。なお、ここでは説明の便宜上、正規アドレス情報提供サーバ59がアドレス発行サーバ60により発行された正規アドレス情報を記憶する場合を示したが、この正規アドレス情報提供サーバ59は、正当な端末である他のアドレス発行サーバや通信機器により発行された正規アドレス情報についても記憶する。たとえば、図中に示す通信機器16が通信機器17等を攻撃するパケットを送出しない正当な装置であると認証されている場合には、正規アドレス情報提供サーバ59は、かかる通信機器16により発行された正規アドレス情報についても記憶する。

【0100】

次に、この分散型サービス不能攻撃防御システム50のシステム構成について説明する。図11に示すように、分散型サービス不能攻撃防御システム50は、ネットワーク2を介して伝送されるパケットを中継する複数の中継装置53～56と、ネットワーク2を介して通信機器7に送信されるパケットの通過を制限するゲート装置58と、ネットワーク2を介した攻撃を行わないパケットの送信元を表す正規アドレス情報を記憶する正規アドレス情報記憶装置59とを備えている。なお、図11に示した分散型サービス不能攻撃防御システム50の構成は、一例を示すものであり、中継装置、およびゲート装置等の数量やネットワーク構成を限定するものではない。

【0101】

ゲート装置58は、ゲートウェイ装置によって構成され、LAN14に接続されている。また、中継装置53～56は、ルータ装置によってそれぞれ構成されている。なお、中継装置53～56は、ブリッジによってそれぞれ構成されていてもよい。

【0102】

ここで、中継装置53は、中継装置54およびゲート装置58に接続され、中継装置54は、通信機器15、中継装置53および正規アドレス情報記憶装置59に接続され、中継装置55は、通信機器16および中継装置56に接続され、中継装置56は、中継装置55、エッジルータ11およびゲート装置58に接続されているものとする。

【0103】

図12は、図11に示したゲート装置58の構成を示すブロック図である。このゲート装置58は、攻撃検知部20と、容疑シグネチャ生成部21と、正規条件情報格納部22と、正規条件情報格納部22に格納される正規条件情報を生成する正規条件情報生成部73と、正規シグネチャ生成部24と、不正シグネチャ生成部25と、パケット制限部26と、容疑シグネチャおよび正規シグネチャを隣接関係にある中継装置3および中継装置6に通知するシグネチャ通知部77と、ネットワークインタフェース28とを備えている。

【0104】

正規条件情報生成部73は、正規アドレス情報の送信を要求する正規アドレス情報送信要求を正規アドレス情報記憶装置59に送信する。正規条件情報生成部73は、正規アドレス情報送信要求に応じて正規アドレス情報記憶装置59によって送信された正規アドレス情報がネットワークインタフェース28に受信された場合に、正規アドレス情報に基づいて正規条件情報を生成し、生成した正規条件情報を以って正規条件情報格納部22に格納された正規条件情報を更新する。なお、正規条件情報生成部73による正規アドレス情報送信要求の送信は、ゲート装置58のオペレータによる起動に応じて行われるようにしてもよく、定期的に行われるようにしてもよい。シグネチャ通知部77は、上記実施例1において説明したゲート装置8を構成するシグネチャ通知部27に対してゲート装置のアドレス情報の通知を行わない点が相違する。

【0105】

図13は、図11に示した中継装置56のブロック図である。なお、ここでは説明の便

宜上中継装置 5 6 の構成を説明するが、中継装置 5 3 ～ 5 5 についても中継装置 5 6 と同様に構成されている。中継装置 5 6 は、入力ポート 3 0 と、スイッチ 3 1 と、出力ポート 3 2 と、不正シグネチャ生成部 3 5 と、バケット制限部 3 6 と、容疑シグネチャおよび正規シグネチャを隣接関係にある中継装置 5 に中継するシグネチャ中継部 8 7 とを備えている。

【 0 1 0 6 】

ここで、シグネチャ中継部 8 7 は、ゲート装置 5 8 を構成するシグネチャ通知部 7 7 と同様に構成されるため、詳細な説明は省略する。なお、中継装置 5 6 は、ゲート装置 5 8 と同様に、攻撃検知部、容疑シグネチャ生成部、正規条件情報格納部、および正規シグネチャ生成部を備えるようにしてもよい。

【 0 1 0 7 】

図 1 1 において、LAN 9 に接続されたアドレス発行サーバ 6 0 は、LAN 9 のアドレス情報、または LAN 9 に接続された通信機器 1 2、1 3 のアドレス情報、すなわち正規アドレス情報を正規アドレス情報記憶装置 5 9 に登録する。

【 0 1 0 8 】

なお、アドレス発行サーバ 6 0 は、正規アドレス情報を定期的に登録するようにしてもよく、アドレス発行サーバ 6 0 のオペレータによる起動に応じて登録するようにしてもよい。また、正規アドレス情報を登録するものとしては、アドレス発行サーバ 6 0 の他にエッジルータ 1 1 等の LAN 9 を構成する装置であれば何れのものでもよい。

【 0 1 0 9 】

以上のように構成された分散型サービス不能攻撃防御システム 5 0 について、図 1 4 を用いてその動作を説明する。なお、ゲート装置 5 8 の攻撃検知動作、中継装置 5 3 ～ 5 6 のシグネチャ受信動作、ゲート装置 5 8 のバケット制限動作については、実施例 1 において図 7 ～ 図 9 を参照して説明したものと同様であるため説明を省略する。

【 0 1 1 0 】

図 1 4 は、本実施例 2 に係る分散型サービス不能攻撃防御システム 5 0 の正規条件情報更新動作を示すシーケンス図である。まず、アドレス発行サーバ 6 0 から送信された正規アドレス情報が正規アドレス情報提供サーバ 5 9 に格納される（ステップ S 4 1）。ゲート装置 5 8 の正規条件情報生成部 7 3 によって正規アドレス情報送信要求が正規アドレス情報記憶装置 5 9 に向けて送信されると（ステップ S 4 2）、正規アドレス情報送信要求に回答して正規アドレス情報記憶装置 5 9 から正規アドレス情報がゲート装置 5 8 に向けて送信される（ステップ S 4 3）。

【 0 1 1 1 】

正規アドレス情報がゲート装置 5 8 のネットワークインタフェース 2 8 に受信されると、受信された正規アドレス情報に基づいて正規条件情報が正規条件情報生成部 7 3 によって生成され（ステップ S 4 4）、生成された正規条件情報を以って正規条件情報格納部 2 2 に格納された正規条件情報が更新される（ステップ S 4 5）。

【 0 1 1 2 】

以上説明したように、分散型サービス不能攻撃防御システム 5 0 によれば、ネットワーク 2 を介した攻撃を行わないバケットの送信元を表す正規アドレス情報がゲート装置 5 8 からの要求に応じて送信され、ゲート装置 5 8 に送信された正規アドレス情報に基づいて、通信機器 7 に対する攻撃とみなされないバケットの条件を表す正規条件情報を更新するため、正規条件情報を容易に管理することができる。

【 0 1 1 3 】

なお、上記実施例 1 および 2 に示したゲート装置は、コンピュータにプログラムをロードして実行することにより機能発揮する。具体的には、コンピュータの ROM（Read Only Memory）等に正規アドレス情報を取得するルーチン、正規アドレス情報に基づいて非攻撃バケットの条件を示す正規条件情報を生成するルーチン、ネットワークから受信したバケットのうち正規条件情報に示された条件に適合するバケットの通過を許容しつつ、通信機器へ攻撃をおこなうバケットの通過を制限するルーチンを含むプログラムを記憶してお

き、かかるプログラムをCPUにロードして実行することにより、本発明に係るゲート装置を形成することができる。

【産業上の利用可能性】

【0114】

以上のように、本発明にかかるサービス不能攻撃防御方法、サービス不能攻撃防御装置、中継装置、サービス不能攻撃防御プログラムおよび中継装置用プログラムは、サービス不能攻撃および分散型サービス不能攻撃から通信機器を防御する場合に適している。

【図面の簡単な説明】

【0115】

【図1】本実施例1に係る分散型サービス不能攻撃防御システムの構成を示すブロック図である。

【図2】図1に示したゲート装置の構成を示すブロック図である。

【図3】本実施例1に係る攻撃検知条件の一例を示す図である。

【図4】本実施例1に係る正規条件情報の一例を示す図である。

【図5】本実施例1に係る不正条件の一例を示す図である。

【図6】図1に示した中継装置の構成を示すブロック図である。

【図7】図2に示したゲート装置の攻撃検知動作を示すフローチャートである。

【図8】図6に示した中継装置のシグネチャ受信動作を示すフローチャートである。

【図9】図2に示したゲート装置のバケット制限動作を示すフローチャートである。

【図10】本実施例1に係る分散型サービス不能攻撃防御システムの正規条件情報更新動作を示すシーケンス図である。

【図11】本実施例2に係る分散型サービス不能攻撃防御システムの構成を示すブロック図である。

【図12】図11に示したゲート装置の構成を示すブロック図である。

【図13】図11に示した中継装置の構成を示すブロック図である。

【図14】本実施例2に係る分散型サービス不能攻撃防御システムの正規条件情報更新動作を示すシーケンス図である。

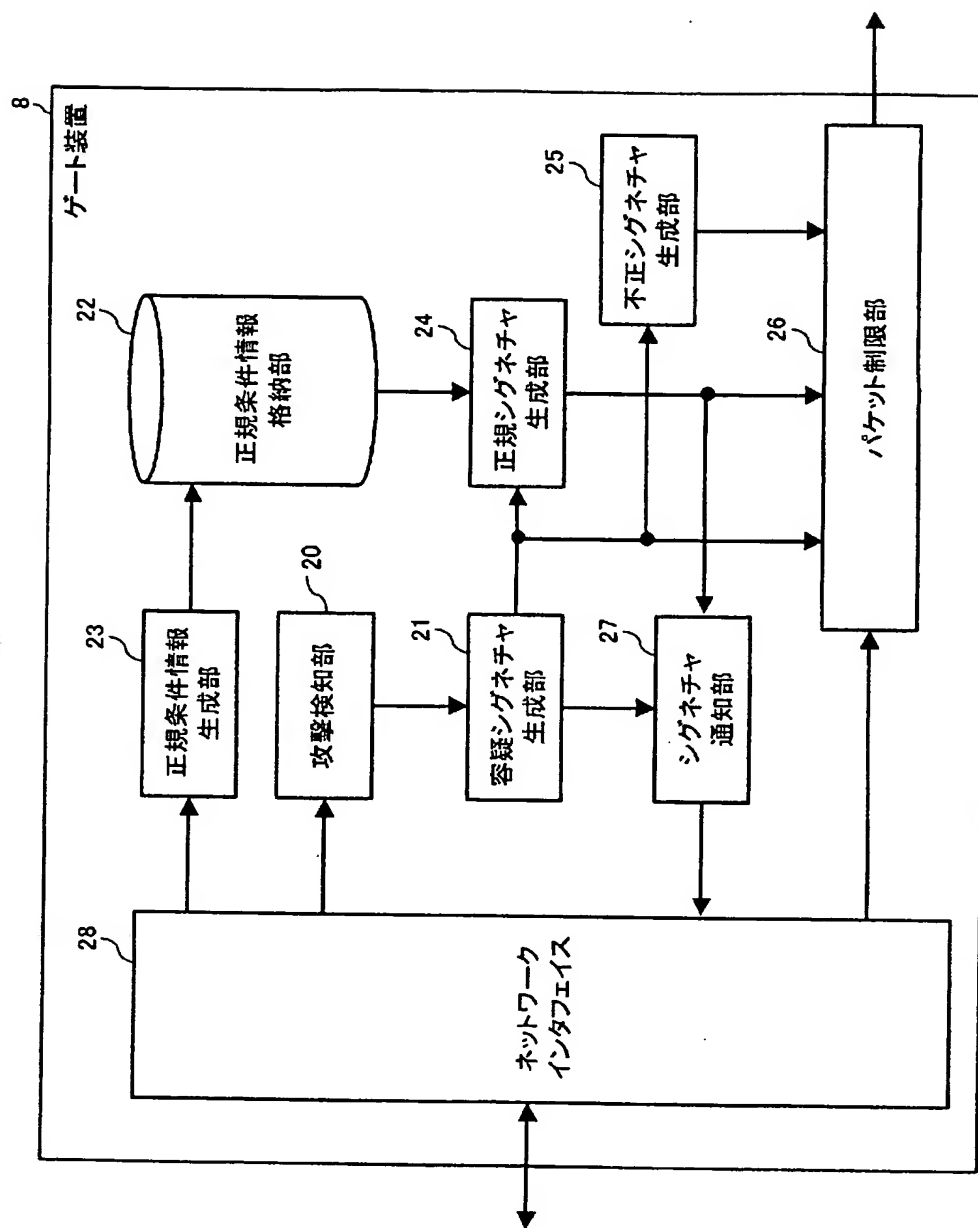
【符号の説明】

【0116】

- 1、50 分散型サービス不能攻撃防御システム
- 2 ネットワーク
- 3、4、5、6、53、54、55、56 中継装置
- 7 通信機器
- 8、58 ゲート装置
- 9 LAN
- 10、60 アドレス発行サーバ
- 11 エッジルータ
- 12、13、15、16 通信機器
- 14 LAN
- 20 攻撃検知部
- 21 容疑シグネチャ生成部
- 22 正規条件情報格納部
- 23、73 正規条件情報生成部
- 24 正規シグネチャ生成部
- 25、35 不正シグネチャ生成部
- 26、36 バケット制限部
- 27、77 シグネチャ通知部
- 37、87 シグネチャ中継部
- 28 ネットワークインタフェース
- 30 入力ポート

- 3 1 スイッチ
- 3 2 出力ポート
- 3 8 アドレス情報記憶部
- 3 9 正規アドレス情報送信部
- 5 9 正規アドレス情報記憶装置

【図 2】



【図 3】

	検知属性	検知閾値	検出時間
1	[Dst=192.168.1.1/32, Protocol=TCP, Port=80]	500kbps	10秒
2	[Dst=192.168.1.2/32, Protocol=UDP]	300kbps	10秒
3	[Dst=192.168.1.0/24]	1Mbps	20秒

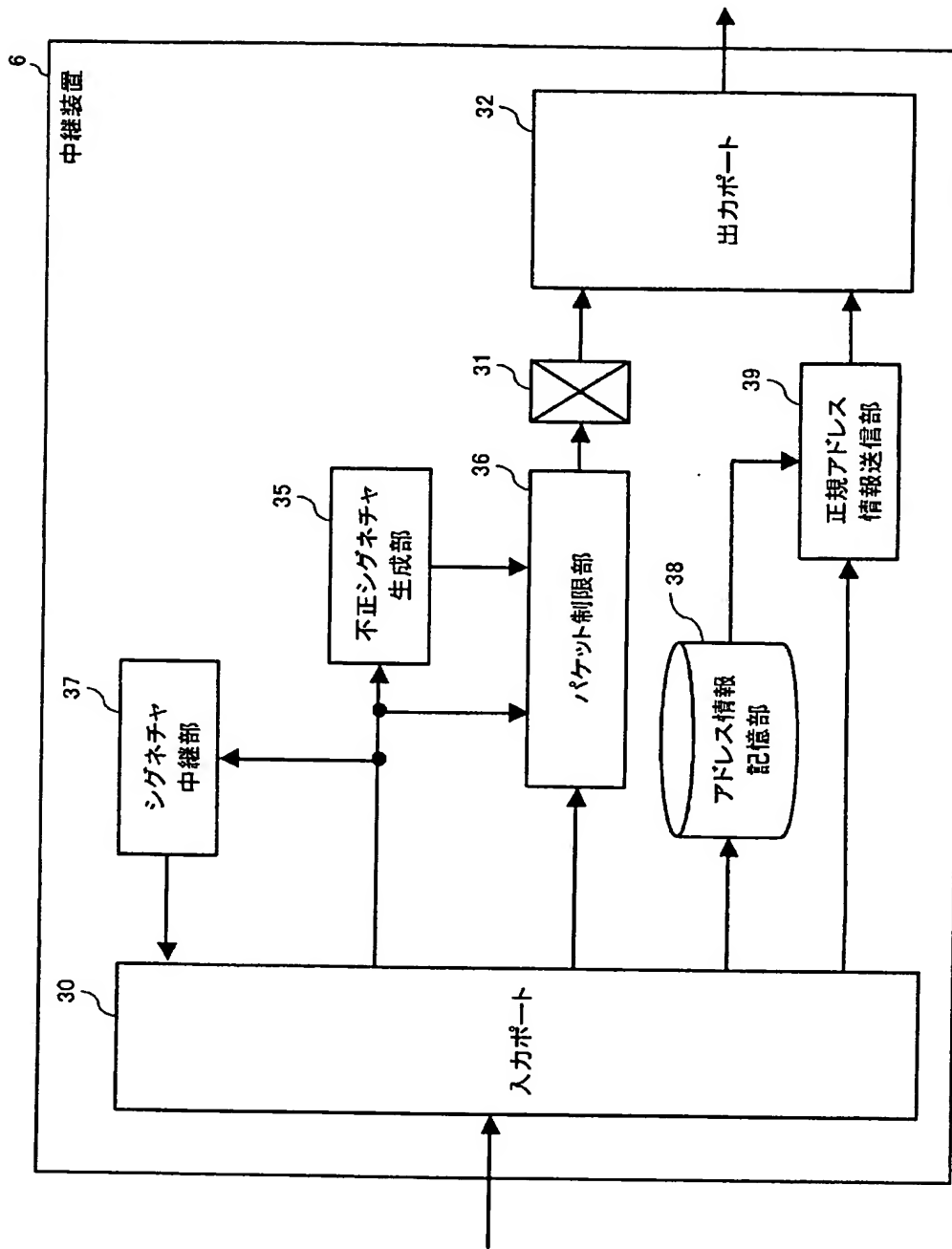
【図 4】

	正規条件
1	{Src=172.16.10.0/24}
2	{TOS=0x01}

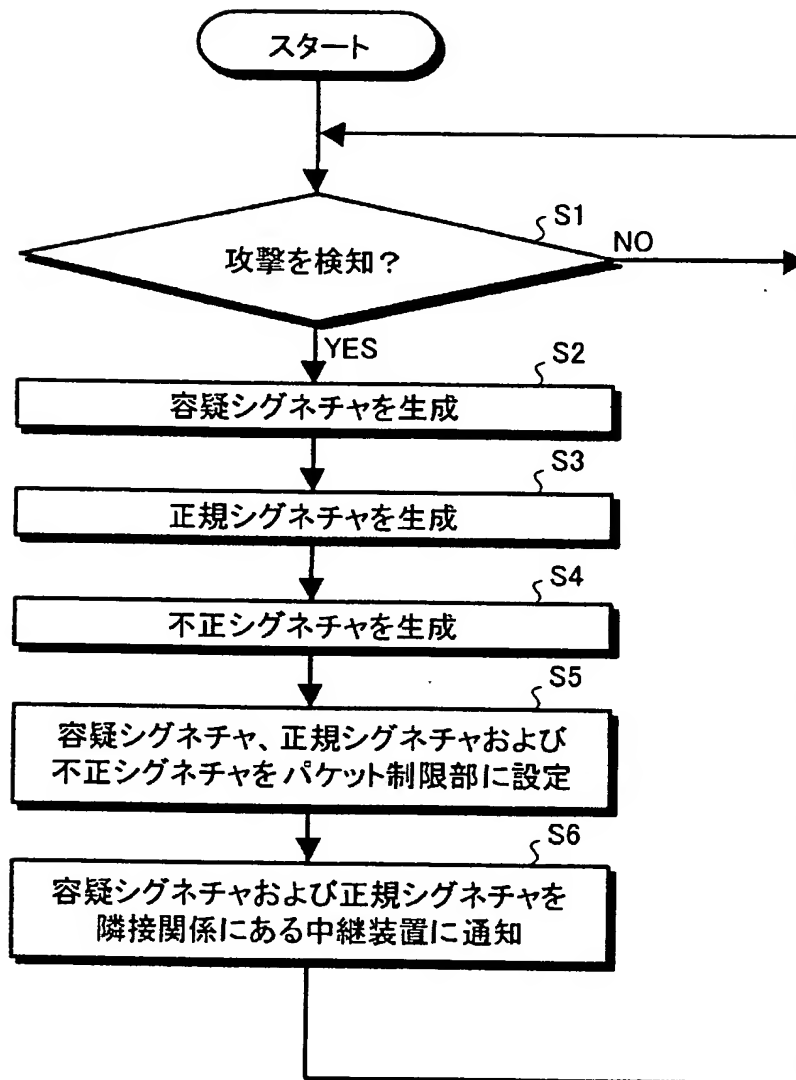
【図 5】

	不正条件
1	500kbps以上のパケットが30秒以上連続送信されている
2	300kbps以上のICMP/Echo Replyパケットが15秒以上連続送信されている
3	300kbps以上のフラグメントパケットが15秒以上連続送信されている

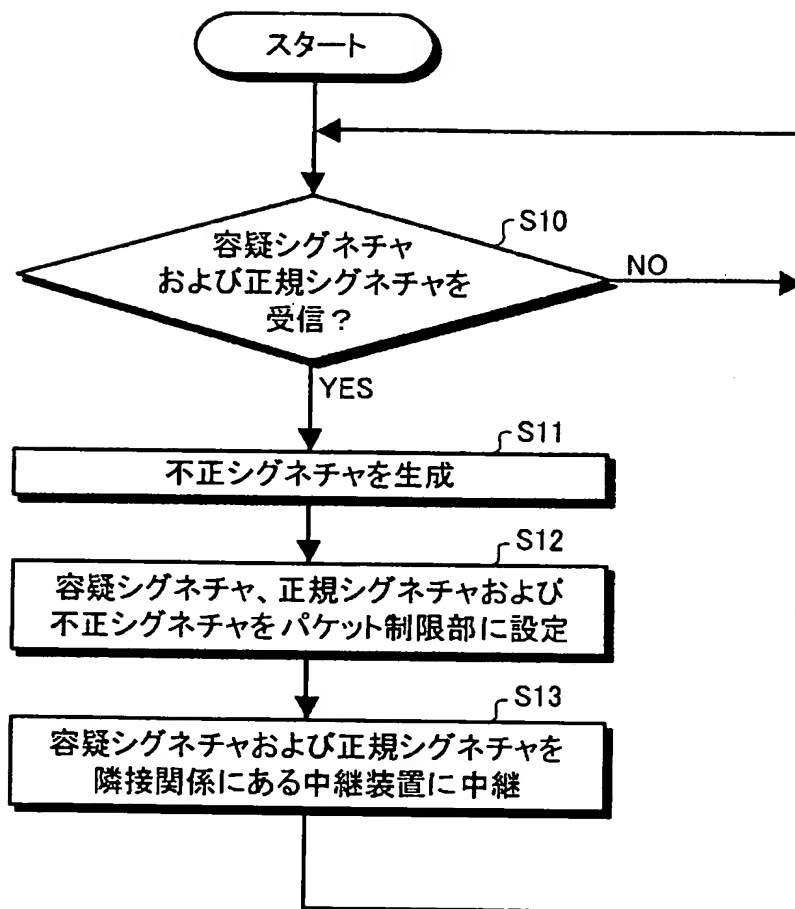
【図 6】



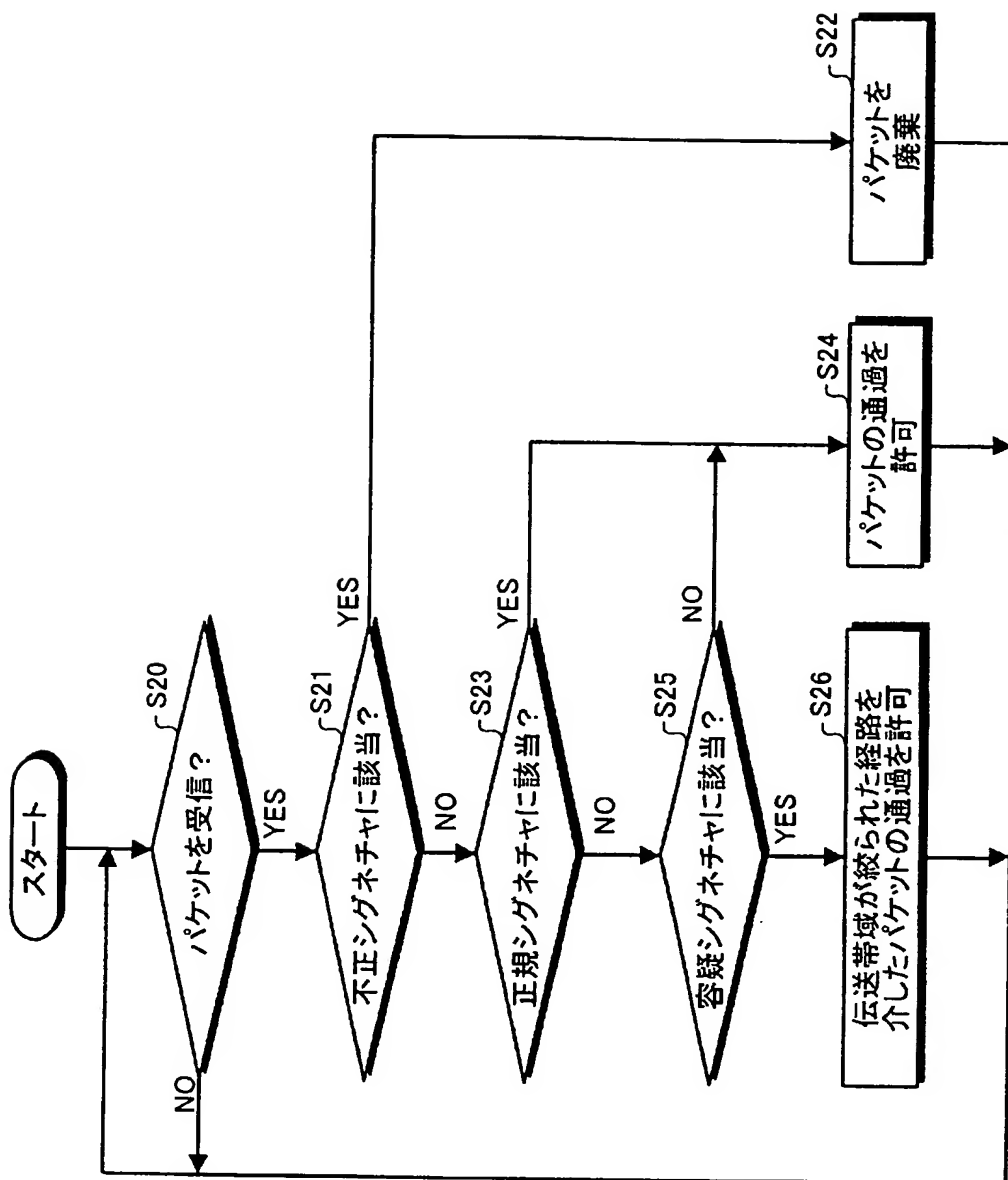
【図 7】



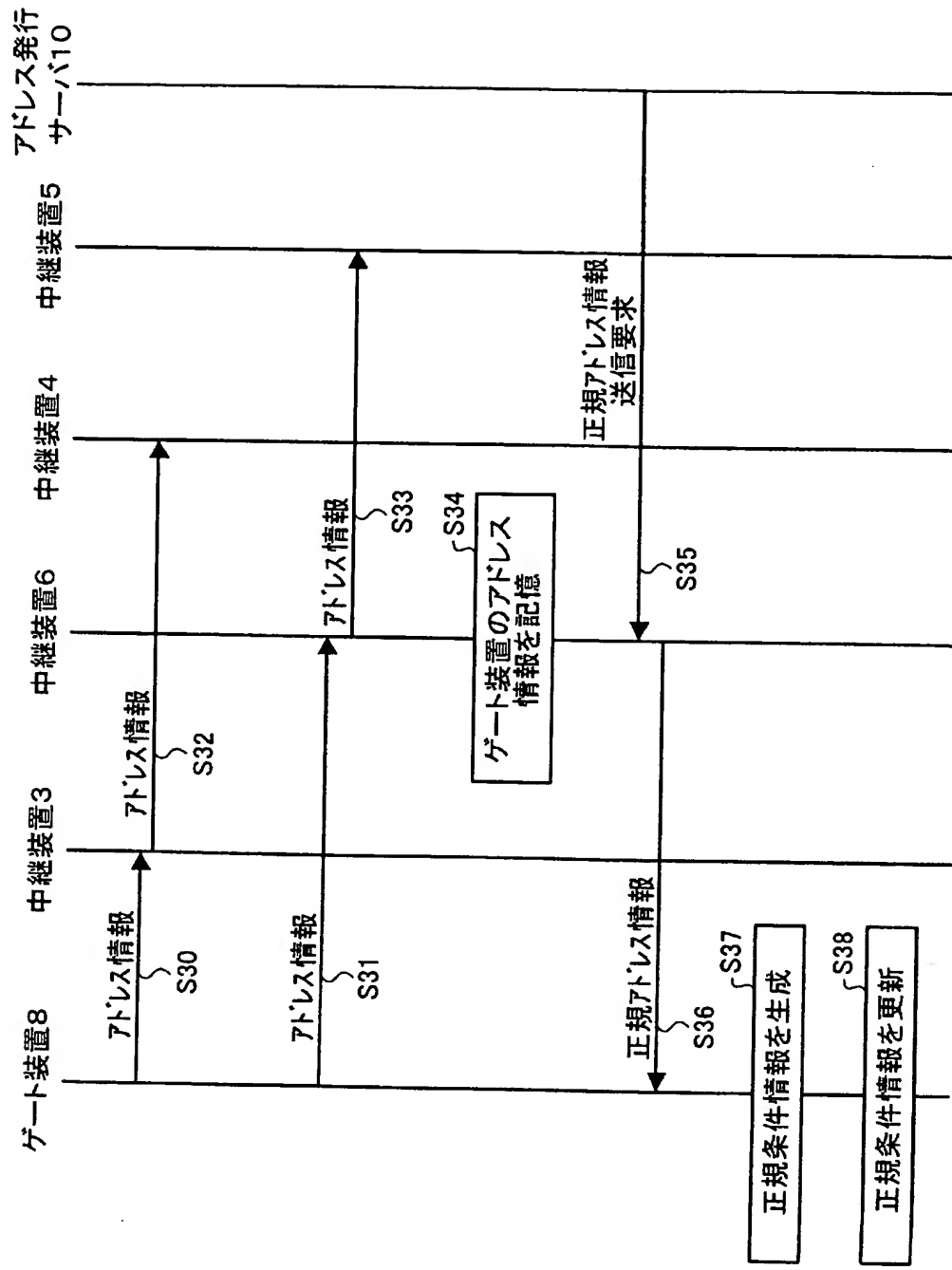
【図 8】



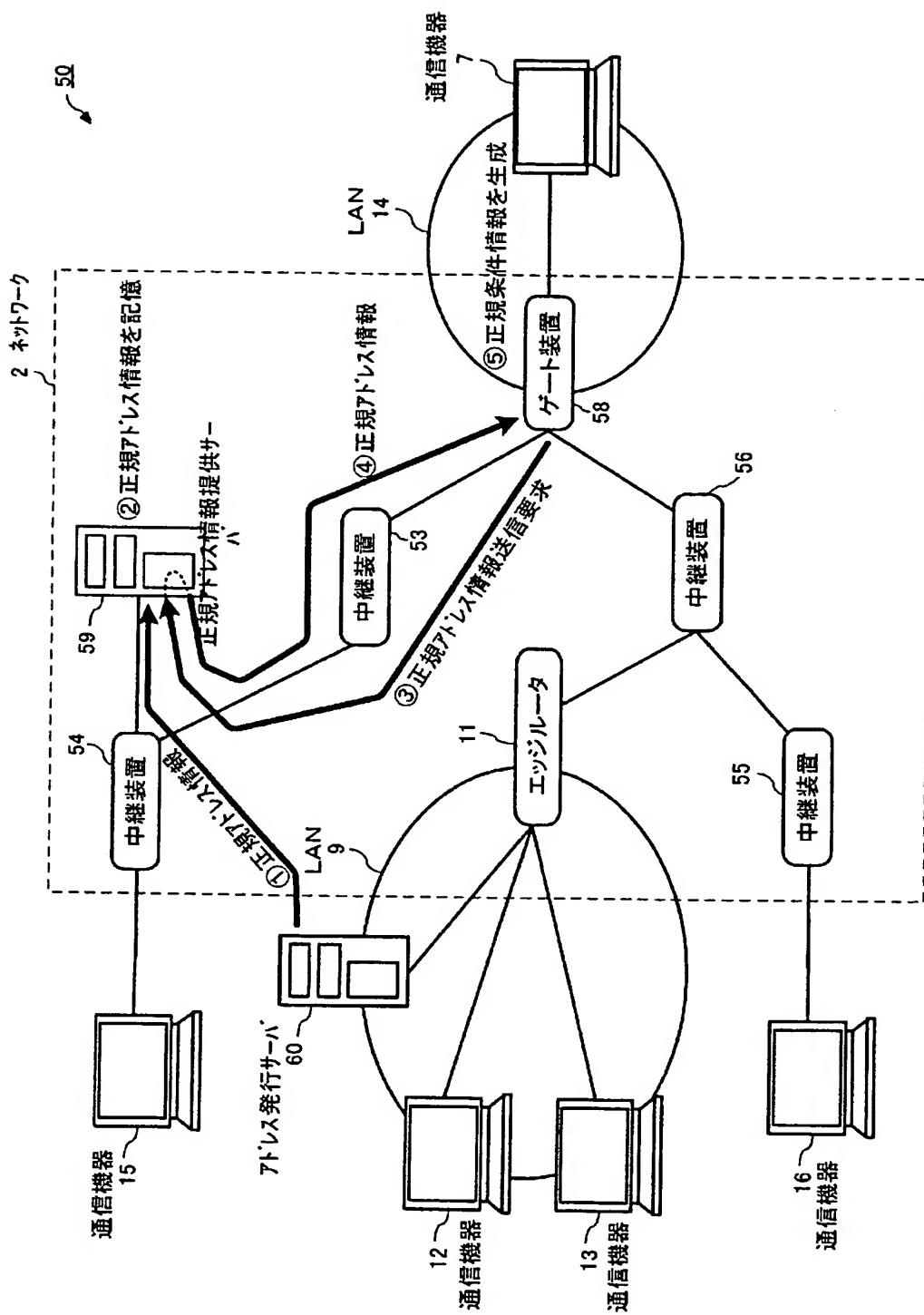
【図 9】



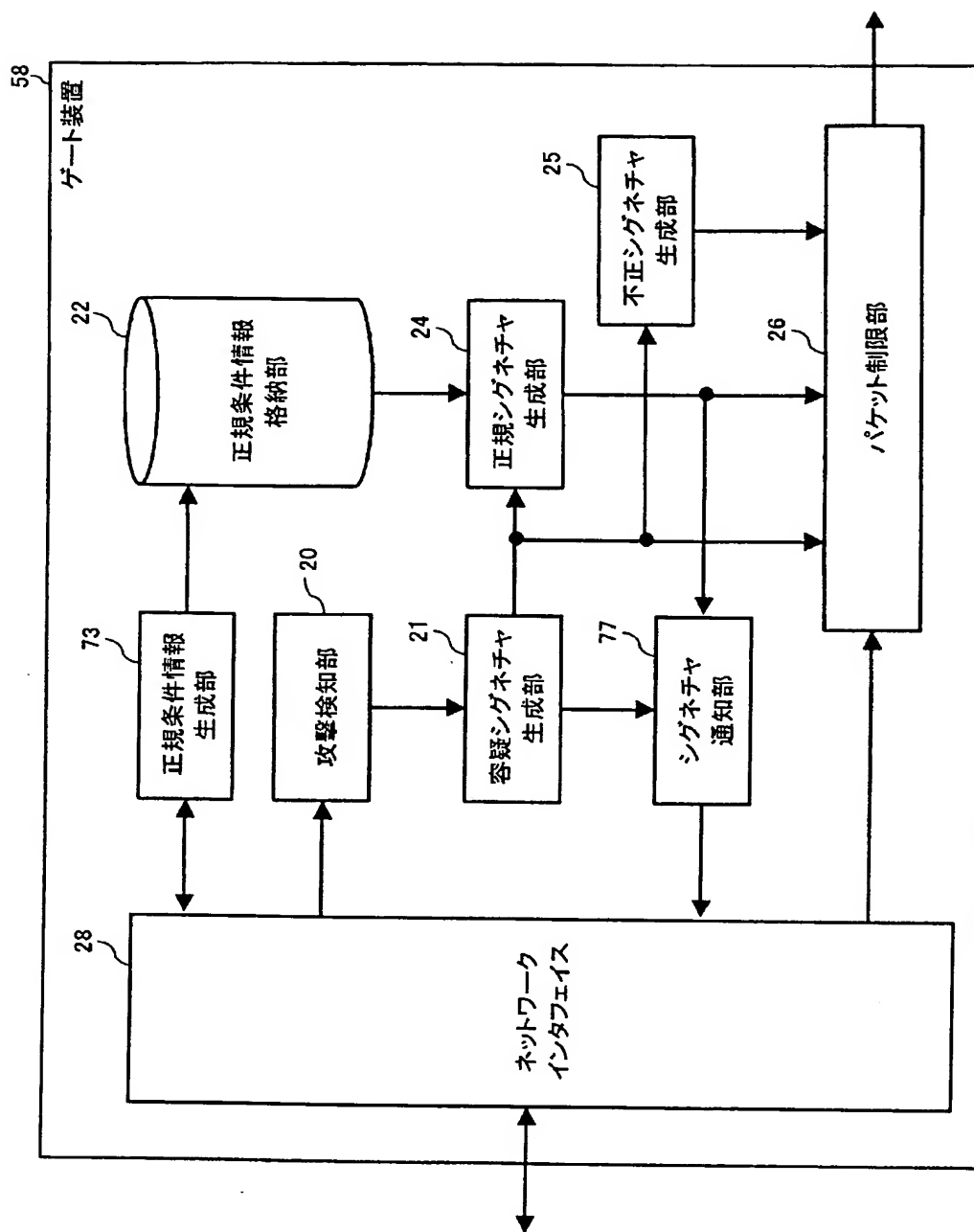
【図 10】



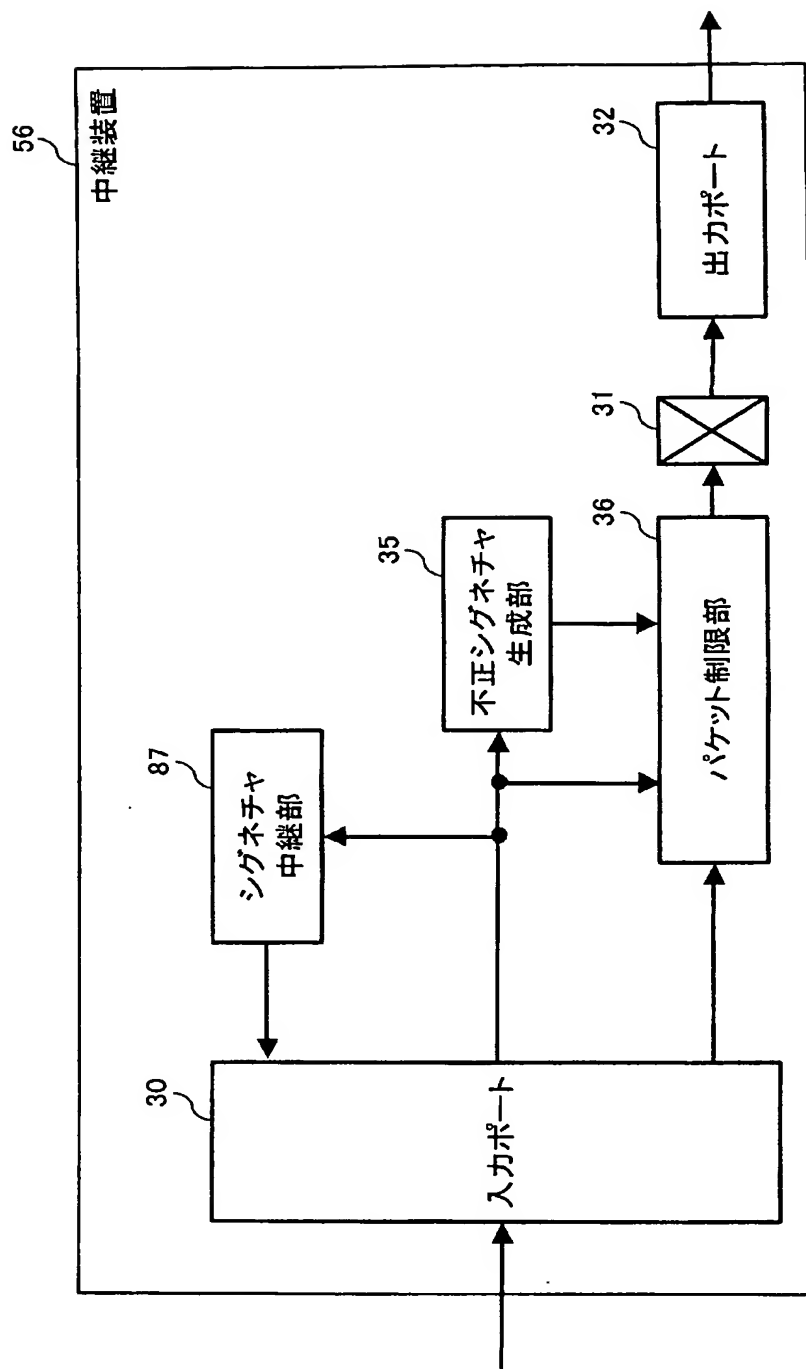
【図 1 1】



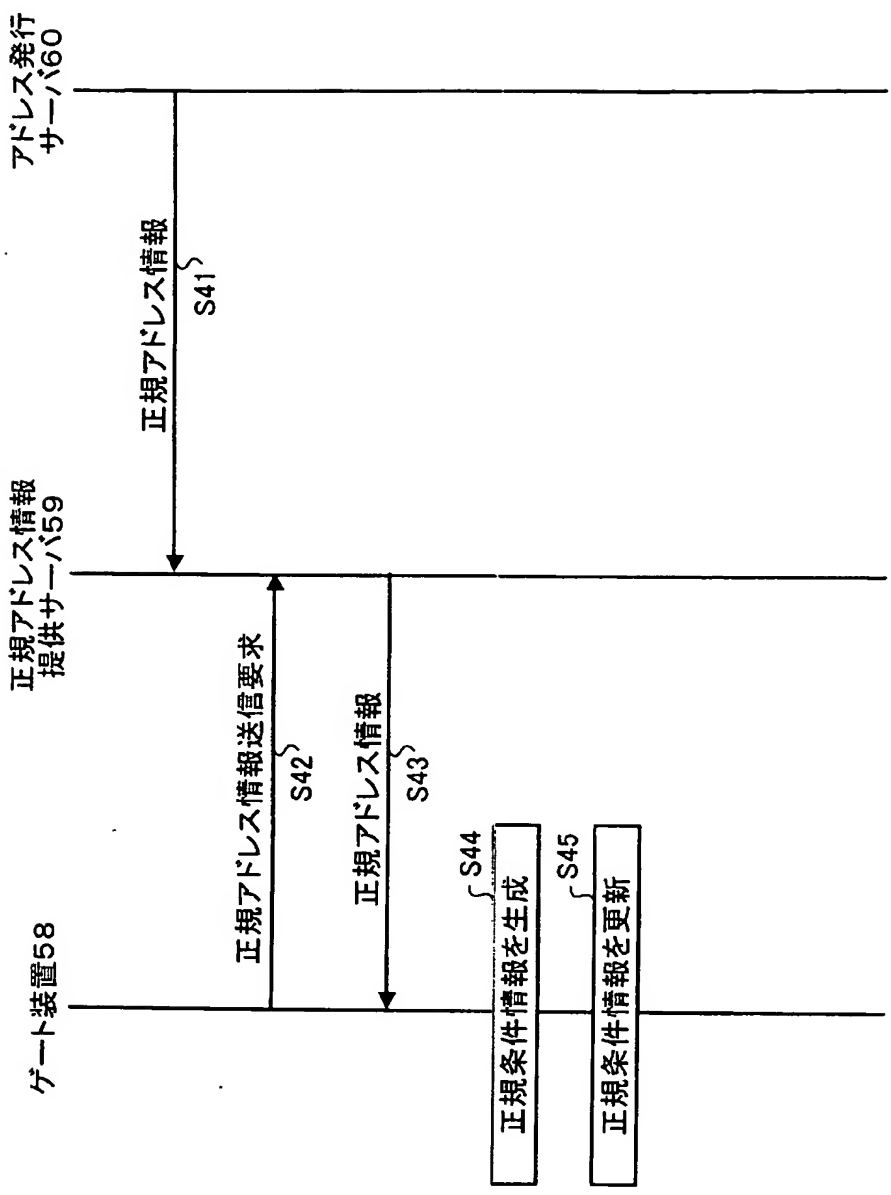
【図 12】



【図 13】



【図 1 4】



【書類名】要約書

【要約】

【課題】 防御対象の通信機器に対して攻撃をおこなわない非攻撃パケットの条件を表す正規条件情報を容易に管理することを課題とする。

【解決手段】 ネットワーク 2 上に所在する正当な装置（アドレス発行サーバ 10）により送信された非攻撃パケットの送信元を示す正規アドレス情報をゲート装置 8 が取得し、取得した正規アドレス情報に基づいてゲート装置 8 が非攻撃パケットの条件を示す正規条件情報を生成し、ネットワークから受信したパケットのうち正規条件情報に示された条件に適合するパケットの通過を許容しつつ、通信機器 7 へ攻撃をおこなうパケットの通過を制限する。

【選択図】

図 1

出願人履歴

0 0 0 0 0 4 2 2 6

19990715

住所変更

5 9 1 0 2 9 2 8 6

東京都千代田区大手町二丁目3番1号
日本電信電話株式会社

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record.**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☒ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.